DOI: 10.17117/na.2015.12.02.107

<http://ucom.ru/doc/na.2015.12.02.107.pdf>

Поступила (Received): 14.12.2015

Кононова Н.В., Хазанов Д.Г. Анонимность, какая она есть

Kononova N.V., Hazanov D.G.
Anonymous, for what it is

При работе в компьютерной сети полная анонимность практически невозможна. Каждый компьютер имеет свой IP-адрес, по которому можно идентифицировать владельца и его действия. Избавиться от него невозможно, так он необходим для маршрутизации данных, а вот прокси-сервер отправляет запросы и получает информацию как бы от себя

During the work in a computer network full anonymity is almost impossible. Each computer has the IP address to which it is possible to identify the owner and his actions. It is impossible to get rid of it, so it is necessary for routing of data, and here the proxy server sends requests and receives information as if from itself

Ключевые слова: анонимность, информационная безопасность, прокси-сервер

Key words: anonymity, information security, proxy-server

Кононова Наталия Владимировна

Кандидат физико-математических наук, доцент
Северо-Кавказский федеральный университет
г. Ставрополь, ул. Индустриальная, 27

Kononova Natalia Vladimirovna

Candidate of Physico-mathematical Sciences,
Associate Professor
North-Caucasus federal university
Stavropol, Industrialnaya st., 27

Хазанов Даниил Геннадьевич

Северо-Кавказский федеральный университет
г. Ставрополь, ул. Индустриальная, 27

Hazanov Daniel Gennadevich

North-Caucasus federal university
Stavropol, Industrialnaya st., 27

– С каких это пор интернет вмешивается
в частную жизнь людей?!
– С 6 августа 1991 года"

Возможна ли полная анонимность в сети? Практически нет. Каждый компьютер имеет свой IP-адрес, по которому можно идентифицировать владельца и его действия. Избавиться от него невозможно, так он необходим для маршрутизации данных, а вот прокси-сервер отправляет запросы и получает информацию как бы от себя. Казалось бы вот она панацея, но не все так просто в следствии того, что подавляющее большинство прокси-серверов в своих запросах передают в специальном поле (x-forwarded-for) IP-адрес конечного пользователя (существуют так называемые анонимные службы, однако их поиск – это очень большая проблема).

Проблема состоит в халатности пользователей к собственной анонимности в глобальной сети, которая ведёт к тому, что информация попадает в третьи руки зачастую без ведома пользователя.

Актуальность проблемы: благодаря разоблачению Эдварда Сноудена общественность стала более информирована о возможностях слежки ФБР и ЦРУ как за простыми юзерами, так и за другими разведывательными компаниями и лидерами стран. На фоне этого проблема скрытия личных данных от чужих глаз в интернете стала актуальной!

Необходимость препятствовать попаданию информации третьим лицам выявила следующие задачи:

1. Обнаружение путей, по которым информация может переходить к третьим лицам.

2. Поиск способов минимизирования потока или вовсе пресечение утечки информации.

Обзор: По данным Яндекса к концу 2014 года численность интернет-пользователей в России составила около 80 млн. человек. И эта цифра растёт. И согласно опросам лишь 10% пользователей задумываются о том, куда идёт вся информация, попадающая, или когда-то попадавшая в интернет.

Выводы: в современном мире, мире красивых гаджетов, в мире умных телефонов, часов и прочей кухонной утвари главное не сдать самого себя им с потрохами. Для этого надо больше следить за тем, что ты выкладываешь в сети.

Когда заходит речь о сетевой безопасности, большое внимание следует уделить всему, что касается анонимности в Интернет. В сознании среднестатистического пользователя интернета бытует следующее мнение: «Для чего мне озадачиваться вопросами анонимности? Я ведь не совершаю никаких противоправных поступков, пусть об этом беспокоятся хакеры...» Однако, давайте задумаемся, насколько комфортно Вы бы себя чувствовали, если бы любой прохожий на улице знал, где Вы проживаете. Кто-то из них наверняка начал бы следить за вами и, несомненно, постарался бы проникнуть к вам домой. Такое положение дел уж точно никому не должно понравиться. Так почему проблеме анонимности в Интернет придают так мало значения? Ответ прост – это пользовательская неграмотность и как с любой неграмотностью с ней нужно бороться.

В наше время социальные сети стали очень модны, мы с радостью делимся с друзьями и знакомыми самыми приятными моментами жизни, но задумываемся ли мы о том, может ли попасть эта информация в «не те руки»? Давайте разберёмся.

Чтобы понять, чего нам бояться, нужно понимать что происходит, когда мы запускаем любимый браузер и вводим адрес любимого сайта. Постараемся проследить весь путь нашей информации в пучине сети.

Первым делом браузер отправляет определенным образом составленный запрос, кусочек данных или пакет. Что же с ним происходит, с этим пакетом?

Сначала ваша операционная система сообщает вашему сетевому устройству, что определенные пакеты хотят покинуть родной браузер и добраться до

xxx.com. Если все условия для этого соблюдены, пакеты покидают ваш компьютер и отправляются по проводам до далекого сервера, а система ждет пока они вернутся.

Покинув компьютер пакеты идут напрямик по воздуху до вашего роутера, если у вас Wi-Fi, а потом до маршрутизатора интернет-провайдера (Частный случай с 3g/4g и т.д. будет рассмотрен ниже).

После этого маршрутизатора пакеты отправляются в главный дата-центр провайдера, который заведует биллингом (хранит и обрабатывает ваши с ним расчеты), учетными записями клиентов и другими базами данных. Именно этот главный дата-центр в большинстве случаев отправит наши пакеты дальше.

Скорей всего у провайдера есть свои собственные dns-сервера (они нужны, чтобы преобразовать красивое xxx.com в понятное компьютерам 141.0.173.173, то есть ip-адрес сервера с искомой информацией) и, прежде чем отправить пакеты дальше провайдер поймет, какой именно сайт нам нужен

Итак, оборудование провайдера отправило наши пакеты и они наконец-то дошли до xxx.com. Конечно же с какого мы IP, какой у нас браузер, операционная система, провайдер и много-много еще чего. Владельцы xxx.com заботливо сохраняют ваши данные в своей базе, чтобы использовать ее для статистики, некоторым людям может не понравиться, что такая информация попадает в третьи руки. Продвинутые машины типа Google, могут очень точно указывать ваши предпочтения, даже если у вас нет аккаунта на Google, а вы просто пользуетесь их поиском. Конечно же, они сохраняют это только для статистики.

Давайте разберем ситуацию по шагам и поймем, кого же нам стоит бояться, от кого скрываться и самое главное как.

Еще раз маршрут нашего пакета от нашего браузера до xxx.com в виде схемы:

Браузер > ОС > Сетевое оборудование > Провайдер > DNS-сервер > Очень много промежуточных серверов > xxx.com

Затем, xxx.com формирует ответ на наш запрос и отправляет его в обратную сторону и если все в порядке отображается сайт. При каждом действии на сайте, таком как переход на другую страницу, отправка форм и т.д., несчастные пакеты повторяют весь путь туда и обратно. И так, пока нам не надоест.

Браузер > ОС > Сетевое оборудование > Провайдер > DNS-сервер > Очень много промежуточных серверов > xxx.com

Long happy end.

В этой совсем короткой части собраны рекомендации, использование которых поможет вам сохранить анонимность и быть в целостности и сохранности.

Мы опишем их немного не в том порядке, в котором описывали наших врагов (браузер, провайдер, etc.), но в порядке, который нам кажется наиболее подходящим по логике.

1. Придерживаться дотехнических рекомендаций.
2. Не держать могущие скомпрометировать вас вещи/данные рядом с собой, не работать на том же компьютере, с которым вы проводите досуг.
3. Не смотреть фильмы, не пользоваться соц. сетями, прочими проприетарными сервисами и приложениями на компьютере, с которого вы работаете.

4. Использовать свободное программное обеспечение, проверенное в децентрализованных лабораториях пентеста на отсутствие уязвимостей.
5. Использовать шифрование. (PGP, OTR, MD5, TRUE CRIPT)
6. Использовать свободные DNS-серверы.
7. Не хранить переписку, логины, пароли.
8. Если специфика вашей работы позволяет, старайтесь работать в людных местах, где вероятность однозначно определить ваше местонахождение меньше.

В апреле 2008 года было предложено включать в список запрещённых материалов конкретные сайты и все российские провайдеры должны будут заблокировать доступ к запрещённому сайту в течение месяца после публикации списка. Поэтому, если не хотите лишних проблем, то пора пересматривать свое беспечное отношение к пользованию Интернетом – научиться скрывать и шифровать свою деятельность в Сети.